

pianificazione e normativa italiana

il piano di sicurezza

- il piano di sicurezza di una organizzazione è un documento che descrive come l'organizzazione affronta i suoi problemi di sicurezza

plan-do-check-act cycle

- approccio ciclico alla pianificazione e alla azione
 - è un approccio generale non legato alla sicurezza
- quattro fasi che si ripetono
 1. Plan
 - Recognize an opportunity and plan a change.
 2. Do
 - Test the change. Carry out a small-scale study.
 3. Check
 - Review the test, analyze the results and identify what you've learned.
 4. Act
 - Take action based on what you learned in the study step: If the change did not work, go through the cycle again with a different plan. If you were successful, incorporate what you learned from the test into wider changes. Use what you learned to plan new improvements, beginning the cycle again.

perché pianificare

- razionalizzare gli interventi
 - la fine di ottenere buoni risultati con spesa contenuta
- condividere gli obiettivi e i processi all'interno dell'organizzazione
 - sinteticamente con i livelli direzionali
 - in forma estesa all'interno del gruppo che si occupa di sicurezza
- mantenere traccia del processo decisionale
 - al fine di individuare dove e perché una certa decisione è stata presa
 - utile in fase di revisione e correzione
- disporre di uno strumento per verificare il raggiungimento degli obiettivi
 - se non so quali azioni sono state prese non posso verificarne l'efficacia
 - se non posso verificarne l'efficacia non riesco a capire se le attività legate alla sicurezza stanno andando nella direzione giusta e se le devo modificare
- predisporre piani finanziari
 - es. allocare i fondi necessari all'implementazione del piano

contenuto (tipico) di un piano di sicurezza

- policy
- stato attuale
 - inventario degli asset e analisi del rischio
- requisiti e vincoli
- contromisure
- piano di rientro
 - piano di applicazione delle contromisure per la transizione dalla situazione attuale a quella identificata come ottimale
- responsabilità
 - dell'applicazione del piano
- piano di revisione
 - del piano di sicurezza
- piano di risposta agli incidenti, business continuity, disaster recovery

policy

- criterio adottato dall'organizzazione in merito alla sicurezza, sicuramente contrattato con la direzione
- tipicamente un documento ad un elevato livello di astrazione
- sin dalla policy si deve trovare un compromesso tra..
 - efficacia, costi, disagio agli utenti, ecc.
 - rigidità dei controlli vs. deterrente e recovery
- deve identificare
 - oggetti (risorse da proteggere), soggetti (utenti utilizzatori), diritti (tipi di accesso)
 - descrizione a livello astratto: es. i dati personali e non il db XYZ
 - obiettivi ad alto livello
 - priorità di certi aspetti rispetto ad altri: es. continuità di certi settori di business, conformità a normative, privacy dei dati, ecc.
 - responsabilità
 - es. un gruppo, i manager, ecc.
 - l'impegno
 - quante risorse operative o finanziarie
- una delle parti più critiche e complesse del piano

stato attuale

- inventario delle risorse dell'organizzazione rilevanti per la sicurezza (i cosiddetti asset)
 - dati
 - utenti
 - apparecchiature
 - servizi
 - eventuali contromisure già presenti
 - con indicazione della criticità e del “rapporto” tra di essi
- è sostanzialmente una analisi dello stato attuale
- **analisi dei rischi** associati ai vari elementi individuati

rischio

- quando una minaccia si concretizza (in un attacco, virus, fault, ecc) si parla di *evento avverso o incidente*
- il *rischio* è una stima della “perdita” legata ad una certo *evento avverso possibile (cioè una minaccia)*
- *elementi*
 - **impatto**: danno, o perdita economica, in caso di incidente
 - **probabilità**: la probabilità che l’incidente si verifichi
 - **controllabilità**: possibilità di controllarne la probabilità o l’impatto

Valutazione quantitativa del rischio

- una analisi quantitativa ha come obiettivo la valutazione economica della perdita
- valore atteso della perdita per una data minaccia
$$\text{perdita attesa (annua)} = \text{probabilità} * \text{impatto}$$

valutazione quantitativa del rischio

- i metodi quantitativi hanno come obiettivo la valutazione economica della perdita attesa media

Bene: autovettura, valore € 20.000

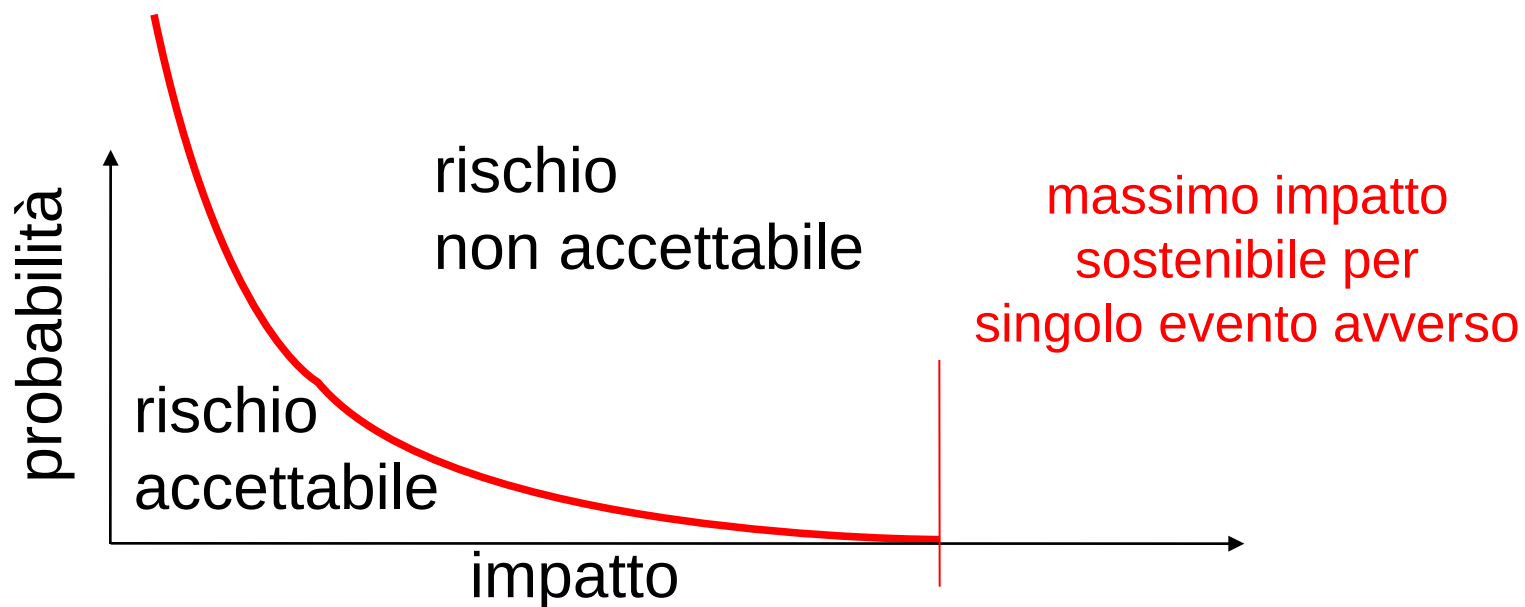
Vulnerabilità : trasportabilità

Minaccia: furto

	senza antifurto	blocca pedali	stellitare
furti su 100000 auto	1000	200	2
probabilità	0,01	0,002	0,00002
impatto economico annuo atteso	€200	€40	€0,4
costo contromisura	-	€12	€300

valutazione del rischio

- c'è una **curva** al di sotto della quale il rischio (perdita attesa annua) è accettabile
- c'è una **soglia** oltre la quale non si può sostenere neanche un singolo incidente, pena il fallimento dell'organizzazione



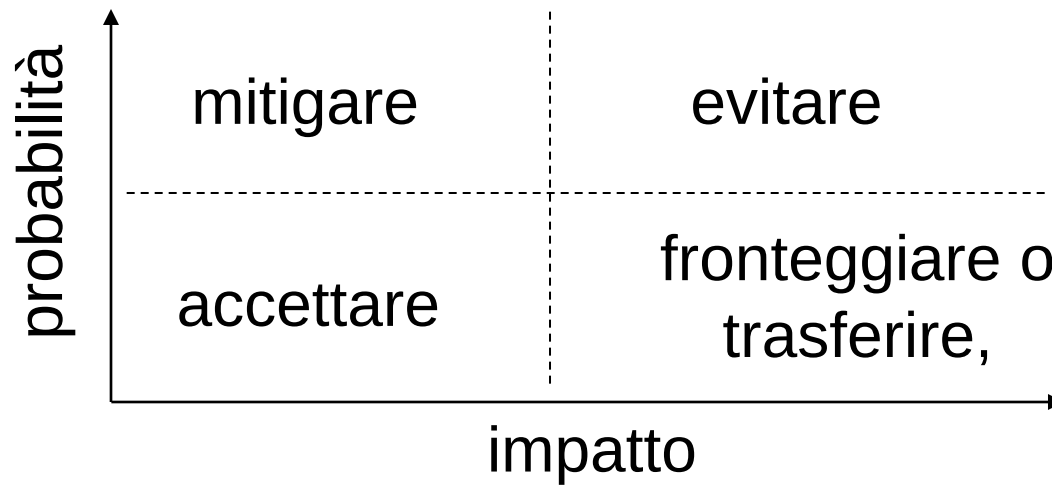
trattamento dei rischi

- a fronte di un rischio possiamo...
 - accettare
 - non facendo nulla se il rischio è sufficientemente basso
 - mitigare
 - inserendo delle **contromisure proattive** di tipo tecnologico, procedurale o organizzativo che riducono la probabilità di evento avverso (es. firewall)
 - fronteggiare
 - preparandoci ad affrontare un incidente inserendo delle **contromisure reattive** di tipo tecnologico, procedurale o organizzativo che ne riducono l'impatto (es. backup)
 - trasferire
 - trasferendo la perdita su un altro soggetto (es. assicurazione o accordi di "mutuo soccorso")
 - evitare
 - non intraprendere l'attività che ci espone al rischio (es. dare l'attività in outsourcing, o cambiare business)

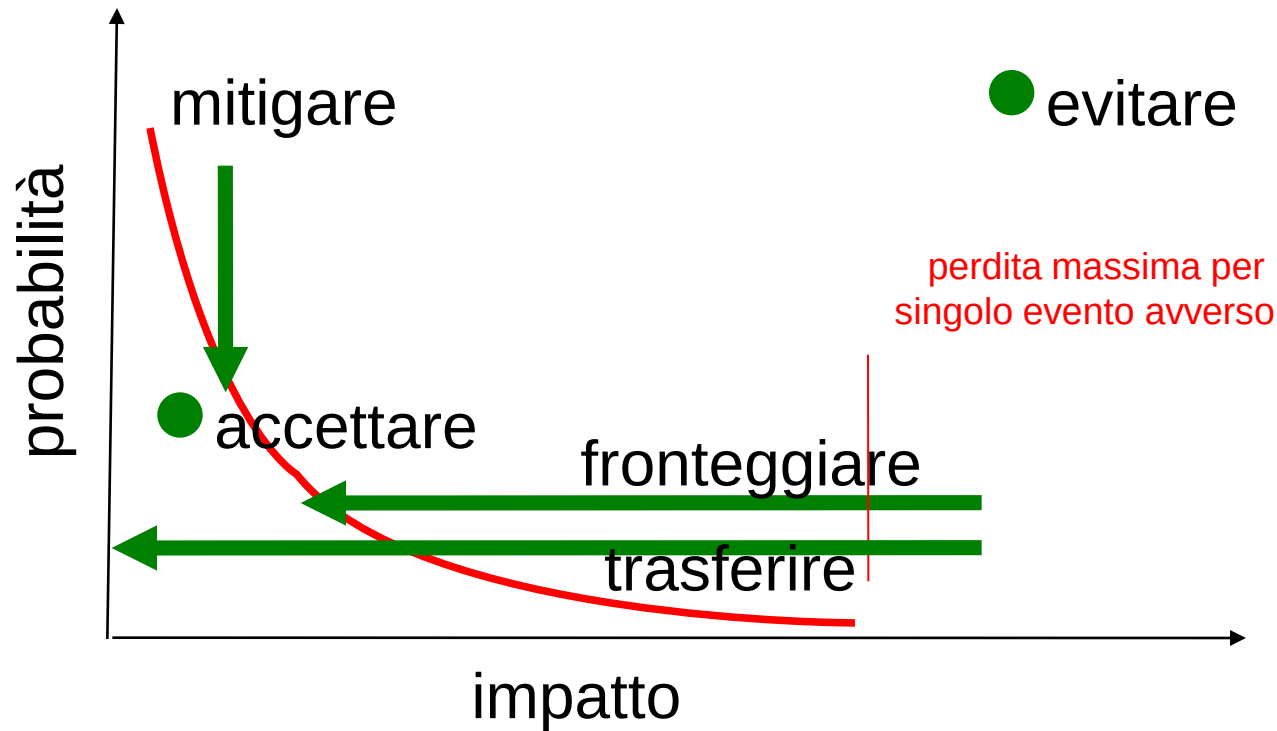
rischi non mitigabili ad alto impatto

- l'evento avverso può non essere mitigabile
 - catastrofi naturali
- se l'impatto del singolo evento avverso è alto non si può sopportare neanche un evento avverso
 - es. per una banca: terremoto con perdita di tutti i dati dei c/c
- ridurre l'impatto fronteggiandolo
 - disaster recovery
 - business continuity

approccio tipico al trattamento dei rischi



approccio tipico al trattamento dei rischi



limiti della valutazione quantitativa

- difficoltà nel monetizzare il valore dei beni
 - es. danni di immagine
- necessità di statistiche e stime di probabilità
 - difficilmente applicabile ad eventi con probabilità molto bassa
- spesso sono usati metodi qualitativi
 - metriche non monetarie
 - es. alto medio basso
 - permettono solo di comparare i rischi tra di loro

requisiti e vincoli

- requisiti
 - identificano ciò che i meccanismi di sicurezza dovranno fare senza specificare come sarà fatto
 - è una descrizione molto più concreta rispetto ad una politica
 - es: deve essere possibile valutare l'efficacia della protezione
 - es: tutti gli utenti che accedono a certi dati devono essere autenticati
 - è una descrizione astratta rispetto al progetto poiché non dice come i requisiti verranno soddisfatti
- vincoli di progetto (o di implementazione)
 - la intranet va protetta con un firewall
 - non si possono usare fingerprint reader

contromisure

- la scelta delle contromisure va fatta in base a
 - costo
 - acquisto di apparati, acquisizione di competenze, consulenze, gestione, manutenzione, aggiornamento, impatto sulla produttività, usabilità, ecc.
 - efficacia
 - di quanto riduce il rischio? ne introduce altri?
 - se gli interventi sono importanti si può prevedere una attività progettuale

responsabilità

- tipicamente la responsabilità della attuazione del piano è distribuita
 - amministratori db
 - responsabili della sicurezza dei db
 - capi progetto
 - responsabili dei dati del loro progetto
 - amministratore di rete
 - responsabile della sicurezza di rete
 - manager
 - responsabili indiretti, cioè responsabili della supervisione delle persone che sono direttamente responsabili della sicurezza
- tipicamente basato sull'organigramma aziendale

roadmap (piano di rientro)

- mostra quali attività vengono effettuate e quando
- dovrebbe...
 - dare precedenza al trattamento dei rischi più importanti
 - diluire l'impegno nel tempo attuando incrementalmente le contromisure più costose e rischiose
 - prevedere eventuali test preliminari (plan-do-check-act) per verificare la sostenibilità delle soluzioni identificate

revisione

- il piano dovrebbe prevedere
 - quando il piano stesso va revisionato
 - ogni anno
 - ogni volta che si installa un nuovo servizio
 - ogni volta che cambia la normativa
 - chi deve fare la revisione del piano
 - revisione fatta internamente
 - revisione in outsourcing

risposta agli incidenti

- può essere parte del piano di sicurezza
- stabilisce procedure in caso di incidente
 - la squadra che si occupa del problema
 - le questioni legali (quando si sporge denuncia)
 - le attività per mantenere le prove (computer forensic)
 - il log delle attività di gestione degli incidenti
 - come condurre le relazioni con l'esterno (es. con i clienti)
- stabilisce cosa fare dopo l'incidente
 - revisione del piano di sicurezza
 - revisione del piano di risposta agli incidenti

bussiness continuity plan e disaster recovery plan

- si occupa di minacce il cui rischio a bassa probabilità e ad alto impatto
 - Epidemie
 - Terremoti
 - Incendi
 - Inondazioni
 - Uragani
 - Interruzione dei servizi (elettricità, acqua, ecc.)
 - Terrorismo
 - Cyber attack

bussiness continuity plan e disaster recovery plan

- requisiti
 - insieme minimo di servizi da mantenere
 - finestra temporale nel quale i servizi devono essere di nuovo disponibili
- la soluzione può prevedere...
 - struttura organizzativa di gestione e comando in caso di crisi
 - procedure di backup e ripristino
 - sito secondario (caldo o freddo)
 - comunicazione tra sito primario e secondario
 - replica dei dati tra primario e secondario
 - servizi disponibili sul sito secondario

normativa sulla privacy

D. Lgs. 196/2003

- trattamento dati personali
- stabilisce
 - figure
 - titolare: la ditta
 - responsabili: dirigenti
 - incaricati: gli impiegati
 - requisiti minimi di sicurezza per i trattamenti informatici
 - redazione del Documento Programmatico di Sicurezza (DPS)
 - molto simile ad un piano di sicurezza ma con l'obiettivo di documentare la conformità al Dlgs 196/2003

196/2003: requisiti minimi di sicurezza (vedi 196/2003 all. B)

- autenticazione

- gli incaricati devono essere tutti autenticati con credenziali (username e password o altro)
 - custodite diligentemente
 - credenziali inutilizzate disattivate entro 6 mesi
- ciascun username è associato a un solo incaricato
 - un incaricato può averne più di uno
- password ≥ 8 caratteri, modificata ogni 6 mesi
 - per i dati sensibili e giudiziari modificata ogni 3 mesi
- accesso in assenza dell'incaricato
- formazione: non lasciare incustodito il terminale

- autorizzazione

- ruoli per classi omogenee di incaricati
 - la consistenza tra ruoli e incaricati va verificata ogni anno
- gli account non usati vanno cancellati

196/2003: requisiti minimi di sicurezza (vedi 196/2003 all. B)

- procedure
 - antivirus e suo aggiornamento ogni 6 mesi
 - i programmi che trattano dati personali comuni aggiornati ogni anno
 - se sensibili o giudiziari ogni 6 mesi
 - backup ogni settimana
 - DPS ogni anno

contenuto del DPS (vedi 196/2003 all. B)

- **elenco dei trattamenti**
- **compiti e responsabilità**
- **analisi dei rischi**
- **contromisure** per garantire integrità, confidenzialità, disponibilità
- **procedure di backup recovery**
- **formazione programmata per gli incaricati al trattamento**
- **cifratura per dati “sensibili”**

196: altri obblighi

- consenso informato
- diritto di accesso, cancellazione
aggiornamento da parte dell'interessato
- comunicazione al “Garante”
 - dati sensibili e altro
- ecc.

155/2005 – norme anti-terrorismo

- detta anche “legge Pisanu”
- chiunque offra un accesso ad Internet deve
 - identificare gli utenti
 - tracciare l’operato degli utenti
 - cioè mantenere log files per eventuali indagini
- ...ma la responsabilità rimane
 - l’identificazione è comunque consigliata per dimostrare il non coinvolgimento in atti illeciti

ABROGATA
dal 1 gen 2011